IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Application Serial No. 10/606,089
Filing Date 06/25/2003
Inventorship ..... Christian et al.
Applicant..... Microsoft Corp.
Group Art Unit..... 2137
Examiner ..... Williams, Jeffery L.
Attorney's Docket No. MS303956.01
Title: Systems and Methods for Declarative Client Input Security Screening

SUPPLEMENTAL APPEAL BRIEF

To: Commissioner for Patents
PO Box 1450
Alexandria, Virginia 22313-1450

From: Richard Bucher (Tel. 509-755-7254; Fax 509-755-7252)
Sadler, Breen, Morasch & Colby
422 W. Riverside Avenue, Suite 424
Spokane, WA 99201

Pursuant to 37 C.F.R. §41.37, Applicant hereby submits a supplemental appeal brief within the requisite time in response to a Notification of Non-Compliant Appeal Brief dated December 18, 2007. The supplemental appeal brief is pursuant to an appeal brief for Application Serial No. 10/606,089, filed June 25, 2003, within the requisite time from the date of filing the Notice of Appeal. Accordingly, Applicant appeals to the Board of Patent Appeals and Interferences seeking review of the Examiner's rejections.

(1) Real Party in Interest

The real party in interest is Microsoft Corporation, the assignee of all right, title and interest in and to the subject invention.

(2) Related Appeals and Interferences

Appellant is not aware of any other appeals, interferences, or judicial proceedings which will directly affect, be directly affected by, or otherwise have a bearing on the Board's decision to this pending appeal.

(3) Status of Claims

Claims 2, 3, 13-15, 22 and 23 are canceled. Claims 1, 4-12, 16-21 and 24-28 are pending and are the subject of this appeal. Claims 1, 4-12, 16-21 and 24-28 are set forth in the Appendix of Appealed Claims on Page 24.

(4) Status of Amendments

The most recent final Office Action has a notification date of May 29, 2007. No amendments were made thereafter.

A Notice of Appeal was filed on August 29, 2007.

(5) Summary of Claimed Subject Matter

A concise explanation of each of the independent claims is included in this Summary section, including specific reference characters, if any. These specific reference characters are examples of particular elements of the drawings for certain embodiments of the claimed subject matter and the claims are not limited to solely the elements corresponding to these reference characters.

With regard to claim 1, a method comprises receiving data input through a web page from a client device (Fig. 3 (304), Page 9 (lines 11-20)); referencing a declarative module to determine a client input security screen to apply to the data input from the client device, wherein the declarative module comprises: a global section that includes at least one client input security screen that applies to any type of client input value (Fig. 2 (234), Fig. 3 (306), Page 8 (lines 3-13), Page 9 (line 13) through Page 10 (line 8)); and an individual values section that includes at least one client input security screen that applies to a particular type of client input value (Fig. (236) Fig. 3 (314), Page 8 (lines 14-23), Page 10 (lines 9-14)); and applying multiple client input security screens to the data input from the client device (Fig. 2 (232), Fig. 3 (304-311), Page 9 (line 7) through Page 12 (line 12)), including at least one client input security screen from the global section of the declarative module and at least one client input security screen from the individual values section of the declarative module (Fig. 2 (232), Fig. 3 (306, 314), Page 8 (line 3) through Page 9 (line 5)), wherein the client input security screens are distinct from one another, and wherein said act of referencing comprises first using the global section to screen one or more client input values and then using the individual values section to screen at least one of said one or more client input

values (Fig. 2 (234, 236), Fig 3 (306-322), Page 9 (line 7) through Page 12 (line 12)).

With regard to claim 12, a system, comprises a web page server unit configured to provide one or more web pages to one or more client devices over a distributed network (Fig. 1 (100, 102), Page 6 (lines 4-7), Fig. 2 (200), Page 7 (lines 4-15)); means for receiving client input data (Fig. 2 (206), Page 7 (lines 4-15), (Fig. 3 (304), Page 9 (lines 11-20)); a declarative module configured to include multiple client input security screens that declare screening rules for client input, wherein the declarative module comprises: a global section that includes one or more client input security screens that are applied to all types of client input (Fig. 2 (234), Fig. 3 (306), Page 8 (lines 3-13), Page 9 (line 13) through Page 10 (line 8)); and an individual values section that includes one or more client input security screens that are applied to specified types of client input (Fig. (236) Fig. 3 (314), Page 8 (lines 14-23), Page 10 (lines 9-14)); and a client input security screening unit (Fig. 2 (232,), Fig. 3 (306, 314), Page 8 (line 3) through Page 9 (line 5)) configured to apply the screening rules for client input to the client input data and to perform one or more actions on invalid client input data, wherein the screening rules are from distinct client input security screens from the global section and the individual values section, and wherein the client input security screening unit is configured to first use the global section to screen one or more client input values and then use the individual values section to screen at least one of said one or more client input values (Fig. 2 (234, 236), Fig 3 (306-322), Page 9 (line 7) through Page 12 (line 12)).

With regard to claim 21, one or more computer-readable storage media (Page 13 (line 11) through Page 14 (line 19)) containing computer-executable instructions that, when executed on a computer, implement a method comprising serving a web page to a client over a distributed network (Fig. 1 (102), Page 6 (lines 4-7), Fig. 2 (200), Page 7 (lines 4-15)); receiving client input via the web page (Fig. 2 (206), Page 7 (lines 4-15), (Fig. 3 (304), Page 9 (lines 11-20)); comparing the client input with multiple and distinct client input security screens stored in a security declarative module (Fig. 2 (232), Fig. 3 (304-311), Page 7 (line 3) through Page 9 (line 5), Page 10 (lines 12-14)), wherein the security declarative module includes a global section configured to screen all types of client input values and an individual values section configured to screen particular types of client input values, wherein the global section is used to first screen one or more client input values (Fig. 2 (234), Fig. 3 (306), Page 8 (lines 3-13), Page 9 (line 13) through Page 10 (line 8)); and then the individual values section is used to screen at least one of the one or more client input values (Fig. (236) Fig. 3 (314), Page 8 (lines 14-23), Page 10 (lines 9-14)); if invalid client input is detected, performing a screening action on the invalid client input as indicated by the security declarative module (Fig. 3 (310, 316), Page 10 (lines 5-8), Page 11 (lines 19-24)); and wherein the client input security screens included in the security declarative module can be applied to multiple web pages (Page 8 (lines 3-13)).

(6) Grounds of Rejection to be Reviewed on Appeal

Claims 1, 4-12, 16-21 and 24-28 stand rejected under 35 U.S.C. § 102(b) as allegedly being anticipated by a publication by David Scott and Richard Sharp entitled "Abstracting Application-Level Web Security" (hereinafter, "Scott").

(7) Argument

The rejections under 35 U.S.C. § 102(b) should be withdrawn because Scott fails to disclose the subject matter of the pending claims. Accordingly, for at least this reason, these claims are allowable.

Claim 1 recites a method, comprising:

- receiving data input through a web page from a client device;
- referencing a declarative module to determine a client input security screen to apply to the data input from the client device, wherein the declarative module comprises:
- a global section that includes at least one client input security screen that applies to any type of client input value; and
- an individual values section that includes at least one client input security screen that applies to a particular type of client input value; and
- applying multiple client input security screens to the data input from the client device, including at least one client input security screen from the global section of the declarative module and at least one client input security screen from the individual values section of the declarative module, wherein the client input security screens are distinct from one another, and wherein said act of referencing comprises first using the global section to screen one or more client input values and then using the individual values section to screen at least one of said one or more client input values.

In making out its rejection, the Office argues that Scott discloses all of the subject matter of claim 1. In this regard, the Office relies on Page 3 (Col. 2 – Para. 2) of Scott for disclosing "referencing a declarative module…" as claimed, Fig. 2 and Page 6 (Col. 1 – Paras. 1-2) for disclosing "a global section…" as claimed and Section 3.4 (Para. 3) for disclosing "…wherein said act of referencing comprises first using the global section … and then using the individual values section …" as claimed.

Applicant respectfully disagrees and traverses this rejection. In this regard, Applicant submits that the Office has mischaracterized the Scott reference, which not only fails to disclose all the subject matter recited in this claim, but actually teaches away from it.

First, Page 3 (Col. 2 – Para. 2) of Scott merely describes a *policy compiler* responsible for generating SPDL code which is loaded into a *security gateway* which acts as a firewall. Missing is any discussion of "referencing a declarative module…" as claimed. As such, Applicant submits that the Office's reliance on this excerpt is misplaced.

Second, Fig. 2 and Page 6 (Col. 1 – Paras. 1-2) of Scott simply fail to disclose "a global section…" as claimed. Specifically, with respect to Fig. 2, this figure shows a DTD specifying two ***individual types of client values*** nested under the policy element, namely a URL type ("Element URL" which in turn has a URL-parameter type: "Element parameter" nested under it) and a cookie type ("Element cookie" nested under "Element URL"). In this regard, the URL-parameter type and the cookie type each are shown as potentially having a validation type ("Element validation") and transformation type ("Element transformation") nested below them. Since Fig. 2, at best, shows two ***individual types of client values***, neither the nested transformation type (for individual client value types URL-parameter and cookie) nor any other feature shown in Fig. 2 can be said to disclose "a global section … that applies to ***<u>any</u> type of client input***" as this is understood in the context of the claim language (e.g., "a global section … and an individual values section…") or in the context of the subject application. (emphasis added).

In this regard, and by way of example and not limitation, the Office is directed to page 9 (lines 16-20) of the subject application which describes "all types of input values" screened by "a global screening portion". This excerpt is reproduced below for the Office's convenience:

> As previously stated, the global screening portion 234 screen all types of input values: ***URL parameters, header values, form values and cookies***. Therefore, any screened values will be screened from all these types of values in the global screening portion 234.
> (emphasis added)

Furthermore, with respect to Page 6 (Col. 1 – Paras. 1-2), this excerpt merely describes the two ***individual types of client values*** identified in the DTD shown in Fig. 2 (i.e., the URL-parameter and cookie client value types). Accordingly, for the reasons given above, this excerpt cannot be said to disclose "a global section … that applies to ***any type of client input***" either. (emphasis added).

Finally, even if Scott did disclose "a global section…" as claimed, which it does not, Section 3.4 fails to disclose "…***first using the global section***" as claimed - and instead actually teaches away from this subject matter. Specifically, and as Applicant explained in its last response (dated March 27, 2007), Paras. 1-3 of Section 3.4 describe Fig. 4, which depicts an algorithm that ***first*** checks parameters and cookies (which the Office equates with an ***individual values section*** (see Office Action, Page 3)), ***then*** applies transformations (which the Office equates with a ***global section*** (see Office Action, Page 3)), and ***finally*** evaluates all expressions (which the Office equates with an individual values section (see Office Action, Page 3)). Accordingly, by teaching an algorithm that ***first*** checks parameters and cookies and ***then*** applies transformations, Fig. 4 and

Paras. 1-3 teach directly away from "…***first using the global section***". As such, the Office's reliance on Section 3.4 is misplaced

In its last Office Action (dated May 29, 2007), the Office disagrees with this explanation and inexplicably relies exclusively on Para. 3 of Section 3.4 without accounting for Para. 2 which describes what happens with respect to the algorithm (depicted in Fig. 4) ***prior to the subject matter described in Para. 3***. As such, Applicant respectfully submits that the Office has mischaracterized Para. 3 of Section 3.4 by ignoring the proper context in which this paragraph is presented – namely ***first*** checking parameters and cookies (equated with ***individual***), ***then*** applying transformations (equated with a ***global***) and ***finally*** evaluating all validations (equated with ***individual***).

Accordingly, in view of the above discussion, Scott fails to disclose the subject matter of claim 1. Hence, for at least this reason, claim 1 is allowable.

Claims 4-11 depend from claim 1 and are allowable as depending from an allowable base claim. These claims are also allowable for their own recited features which, in combination with those recited in claim 1, are not disclosed by the reference of record.

Additionally, regarding claim 5, which recites "…wherein the declarative module further comprises a web.config file", the excerpts cited by the Office on Pages 1 and 3 of Scott describe a special security policy description language (SPDL) used to write security policies. These excerpts do not disclose or suggest "wherein the declarative module further comprises a web.config file." This is not surprising since, as Applicant noted above, the Office has not provided an explanation as to which specific features from this excerpt it is relying on and

equating with "a declarative module". Accordingly, Applicant respectfully submits that the Office's reliance on these excerpts is misplaced.

Additionally, regarding claims 6 and 7, which recite "… wherein the applying the client input security screen further comprises executing a default action on invalid client input detected by the client input security screen" and "…wherein the applying the client input security screen further comprises executing a specified action on invalid client input detected by the client input security screen, the specified action being specified in the client input security screen" respectively, the excerpts cited by the Office on Pages 3 and 4 of Scott describe validation constraints and transformation rules. These excerpts do not disclose or suggest "executing a default action" or "executing a specified action" as claimed. Unfortunately, the only explanation offered by the Office (directed to claim 6 exclusively) merely indicates that Scott discloses the application of several types of input screening and that actions are performed and transformations applied during the screening. (See Office Action, Page 4).

As such, Applicant is left to guess as to what specific features from Scott the Office is equating with "executing a default action" and "executing a specified action". Nevertheless, after thoroughly scrutinizing these excerpts, Applicant is unable to find any discussion of this subject matter and therefore respectfully submits that the Office's reliance on these excerpts is misplaced.

Additionally, regarding claim 11, which recites [t]he method as recited in claim 9, wherein the action to be taken further comprises removing an entire string that contains the one or more screened values detected in the client input", the excerpts/figure cited by the Office on Pages 6 and 9, and in Fig. 5, of Scott merely

describe/depict transformation(s) and fail to disclose or suggest "…removing an entire string that contains the one or more screened values detected in the client input" as claimed. Accordingly, Applicant respectfully submits that the Office's reliance on these excerpts and figure is misplaced.

Claim 12 recites a system, comprising:

- a web page server unit configured to provide one or more web pages to one or more client devices over a distributed network;
- means for receiving client input data;
- a declarative module configured to include multiple client input security screens that declare screening rules for client input, wherein the declarative module comprises:
- a global section that includes one or more client input security screens that are applied to all types of client input; and
- an individual values section that includes one or more client input security screens that are applied to specified types of client input; and
- a client input security screening unit configured to apply the screening rules for client input to the client input data and to perform one or more actions on invalid client input data, wherein the screening rules are from distinct client input security screens from the global section and the individual values section, and wherein the client input security screening unit is configured to first use the global section to screen one or more client input values and then use the individual values section to screen at least one of said one or more client input values.

In making out its rejection, the Office argues that Scott discloses all of the subject matter of claim 12. In this regard, the Office relies on the same argument that it relies on in rejecting claim 1. In addition, the Office relies on Fig. 1 of Scott for disclosing "a web page server" as claimed.

Applicant respectfully disagrees and traverses this rejection. In this regard, Applicant submits that the Office has mischaracterized the Scott reference, which not only fails to disclose all the subject matter recited in this claim, but actually teaches away from it.

First, as noted above, Page 3 (Col. 2 – Para. 2) of Scott merely describes a *policy compiler* responsible for generating SPDL code which is loaded into a *security gateway* which acts as a firewall. Missing is any discussion of "a declarative module" as claimed. Second, Fig. 2 and Page 6 (Col. 1 – Paras. 1-2) of Scott simply fail to disclose "a global section…" as claimed. Specifically, with respect to Fig. 2, this figure shows a DTD specifying ***two individual types of client values*** nested under the policy element. Neither the nested transformation type (for individual client value types URL-parameter and cookie) nor any other feature shown can be said to disclose "a global section that includes one or more client input security screens that are applied to ***all types of client input*** (emphasis added). Furthermore, with respect to Page 6 (Col. 1 – Paras. 1-2), this excerpt merely describes the two ***individual types of client values*** identified in the DTD shown in Fig. 2 and therefore cannot be said to disclose this subject matter either.

Finally, even if Scott did disclose "a global section…" as claimed, which it does not, Section 3.4 and Fig. 4 describe/depict an algorithm that ***first*** checks parameters and cookies and ***then*** applies transformations. As noted above, this not only fails to teach "… to ***first use the global section***" as claimed, but in point of fact actually teaches directly away from it. (emphasis added). As such, the Office's reliance on Section 3.4 is misplaced.

Accordingly, in view of the above discussion, Scott fails to disclose the subject matter of claim 12. Hence, for at least this reason, claim 12 is allowable.

Claims 16-20 depend from claim 12 and are allowable as depending from an allowable base claim. These claims are also allowable for their own recited features which, in combination with those recited in claim 12, are not disclosed by the reference of record.

Additionally, regarding claims 18 and 19, which recite "[t]he system as recited in claim 17, wherein the screening rule further comprises a default screening action that is applied in the absence of a specified screening action" and "[t]he system as recited in claim 17, wherein the screening rule further comprises a specified screening action that is applied to the screened client input" respectively, the figure (Fig. 5) cited by the Office appears to show transformation rules but fails to show "a default screening action" and "a specified screening action" as claimed. Unfortunately, the explanations offered by the Office merely indicate that "Scott discloses a single screening action that is to be performed, and thus, a default screening action" and "Scott discloses a single specific screening action that is to be performed". (See Office Action, Page 7). Upon close inspection, these explanations appear to equate some unidentified single screening action with both "a default screening action" and "a specified screening action". In addition, these explanations fail to indicate which specific feature(s) from Scott the Office is referring to.

As such, Applicant is effectively left to guess as to which features from Scott the Office is relying on. Nevertheless, after thoroughly scrutinizing this

figure, Applicant is unable to find any depiction of this subject matter and therefore respectfully submits that the Office's reliance on Fig. 5 is misplaced.

Additionally, regarding claim 20, which recites "…wherein the declarative module further comprises a web.config file", the excerpts cited by the Office on Pages 1 and 3 of Scott describe a special security policy description language (SPDL) used to write security policies. These excerpts fail to disclose or suggest "wherein the declarative module further comprises a web.config file." This is not surprising since the Office has not provided any explanation as to which specific features from this excerpt it is relying on and equating with "a declarative module". Accordingly, Applicant respectfully submits that the Office's reliance on these excerpts is misplaced.

Claim 21 recites one or more computer-readable storage media containing computer-executable instructions that, when executed on a computer, perform the following steps:

- serving a web page to a client over a distributed network;
- receiving client input via the web page;
- comparing the client input with multiple and distinct client input security screens stored in a security declarative module, wherein the security declarative module includes a global section configured to screen all types of client input values and an individual values section configured to screen particular types of client input values, wherein the global section is used to first screen one or more client input values and then the individual values section is used to screen at least one of the one or more client input values;
- if invalid client input is detected, performing a screening action on the invalid client input as indicated by the security declarative module; and
- wherein the client input security screens included in the security declarative module can be applied to multiple web pages.

In making out its rejection, the Office argues that Scott discloses all of the subject matter of claim 21. In this regard, the Office relies on the same argument that it relies on in rejecting claim 1. In addition, the Office relies on Fig. 5 and Pages 3, 4 and 6 of Scott for disclosing "if invalid client input is detected, performing a screening action on the invalid client input as indicated by the security declarative module" and on Fig. 1 of Scott for disclosing "computer-readable storage media" as claimed.

Applicant respectfully disagrees and traverses this rejection. In this regard, Applicant submits that the Office has mischaracterized the Scott reference, which not only fails to disclose all the subject matter recited in this claim, but actually teaches away from it.

First, Page 3 (Col. 2 – Para. 2) of Scott merely describes a *policy compiler* responsible for generating SPDL code which is loaded into a *security gateway* which acts as a firewall. Missing is any discussion of "a security declarative module" as claimed. Unfortunately, the Office has not provided an explanation as to which specific features from this excerpt it is relying on and equating with this subject matter. Nevertheless, Applicant has thoroughly searched the entire Scott reference (including Fig. 5 and Pages 3, 4 and 6) and is unable to find any discussion of this subject matter. As such, Fig. 5 and Pages 3, 4 and 6 cannot possibly disclose "if invalid client input is detected, performing a screening … as indicated by the security declarative module" as claimed.

Second, Fig. 2 and Page 6 (Col. 1 – Paras. 1-2) of Scott simply fail to disclose "a global section…" as claimed. Specifically, with respect to Fig. 2, this

figure shows a DTD specifying ***two individual types of client values*** nested under the policy element. Neither the nested transformation type (for individual client value types URL-parameter and cookie) nor any other feature shown in Fig. 2 can be said to disclose "a global section configured to screen ***all types of client input values*** (emphasis added). Furthermore, with respect to Page 6 (Col. 1 – Paras. 1-2), this excerpt merely describes the two ***individual types of client values*** identified in the DTD shown in Fig. 2 and therefore cannot be said to disclose this subject matter either.

Finally, even if Scott did disclose "a global section…" as claimed, which it does not, Section 3.4 and Fig. 4 describe/depict an algorithm that ***first*** checks parameters and cookies and ***then*** applies transformations. As noted above, this not only fails to teach "… to ***first use the global section***" as claimed, but in point of fact actually teaches directly away from it. (emphasis added). As such, the Office's reliance on Section 3.4 is misplaced.

Accordingly, in view of the above discussion, Scott fails to disclose the subject matter of claim 21. Hence, for at least this reason, claim 21 is allowable.

Claims 24-28 depend from claim 21 and are allowable as depending from an allowable base claim. These claims are also allowable for their own recited features which, in combination with those recited in claim 21, are not disclosed by the reference of record.

Additionally, regarding claim 24, which recites "…wherein the security declarative module further comprises a web.config file", the excerpts cited by the Office on Pages 1 and 3 of Scott describe a special security policy description language (SPDL) used to write security policies. These excerpts fail to disclose or

suggest "wherein the declarative module further comprises a web.config file." This is not surprising since the Office has not provided any explanation as to which specific features from this excerpt it is relying on and equating with "a declarative module". Accordingly, Applicant respectfully submits that the Office's reliance on these excerpts is misplaced.

Additionally, regarding claim 26, which recites "…wherein the screening action further comprises a default action that is not required to be specified in a client input security screen", the excerpt cited by the Office on Page 6 of Scott describes certain defined transformations but fails to discuss "a default action that is not required to be specified in a client input security screen." Unfortunately, the Office has not provided any further explanation as to which specific features from this excerpt it is relying on and equating with this subject matter. Nevertheless, after thoroughly scrutinizing this excerpt, Applicant is unable to find any discussion of this subject matter and therefore respectfully submits that the Office's reliance on this excerpt is misplaced.

Conclusion

Scott fails to disclose the subject matter of the pending claims. Accordingly, for at least this reason, these claims are allowable. Accordingly, Applicant respectfully requests that the rejections be overturned and that these claims be allowed to issue.

Respectfully submitted,

Dated: 1/11/2007

/J. Richard Bucher/
J. Richard Bucher
Registration No. 57,971
Sadler, Breen, Morasch and Colby, p.s.
422 W. Riverside Ave., Suite 424
Spokane, WA 99201
509-755-7254

(8) Appendix of Appealed Claims

1. (Previously Presented) A method, comprising:

receiving data input through a web page from a client device;

referencing a declarative module to determine a client input security screen to apply to the data input from the client device, wherein the declarative module comprises:

a global section that includes at least one client input security screen that applies to any type of client input value; and

an individual values section that includes at least one client input security screen that applies to a particular type of client input value; and

applying multiple client input security screens to the data input from the client device, including at least one client input security screen from the global section of the declarative module and at least one client input security screen from the individual values section of the declarative module, wherein the client input security screens are distinct from one another, and wherein said act of referencing comprises first using the global section to screen one or more client input values and then using the individual values section to screen at least one of said one or more client input values.

2. (Canceled).

3. (Canceled).

4. (Previously Presented) The method as recited in claim 1, wherein the particular type of client input value is one of the following types of client input values: query string; server variable; form value; cookie.

5. (Previously Presented) The method as recited in claim 1, wherein the declarative module further comprises a web.config file.

6. (Original) The method as recited in claim 1, wherein the applying the client input security screen further comprises executing a default action on invalid client input detected by the client input security screen.

7. (Original) The method as recited in claim 1, wherein the applying the client input security screen further comprises executing a specified action on invalid client input detected by the client input security screen, the specified action being specified in the client input security screen.

8. (Original) The method as recited in claim 1, wherein a client input security screen further comprises one or more values that may be entered as client input, the one or more values further comprising the only values that may be entered as client input.

9. (Original) The method as recited in claim 1, wherein a client input security screen further comprises one or more screened values that, when detected in the client input, cause an action to be taken on the client input.

10. (Original) The method as recited in claim 9, wherein the action to be taken further comprises removing the one or more screened values detected in the client input.

11. (Original) The method as recited in claim 9, wherein the action to be taken further comprises removing an entire string that contains the one or more screened values detected in the client input.

12. (Previously Presented) A system, comprising:

a web page server unit configured to provide one or more web pages to one or more client devices over a distributed network;

means for receiving client input data;

a declarative module configured to include multiple client input security screens that declare screening rules for client input, wherein the declarative module comprises:

a global section that includes one or more client input security screens that are applied to all types of client input; and

an individual values section that includes one or more client input security screens that are applied to specified types of client input; and

a client input security screening unit configured to apply the screening rules for client input to the client input data and to perform one or more actions on invalid client input data, wherein the screening rules are from distinct client input security screens from the global section and the individual values section, and wherein the client input security screening unit is configured to first use the global

section to screen one or more client input values and then use the individual values section to screen at least one of said one or more client input values.

13. (Canceled).

14. (Canceled).

15. (Canceled).

16. (Original) The system as recited in claim 12, wherein a screening rule further comprises a client input variable that may be accepted as input from a client.

17. (Original) The system as recited in claim 12, wherein a screening rule further comprises one or more screened characters that, when detected in client input, are screened from the client input according to a screening rule.

18. (Original) The system as recited in claim 17, wherein the screening rule further comprises a default screening action that is applied in the absence of a specified screening action.

19. (Original) The system as recited in claim 17, wherein the screening rule further comprises a specified screening action that is applied to the screened client input.

20. (Previously Presented) The system as recited in claim 12, wherein the declarative module further comprises a web.config file.

21. (Previously Presented) One or more computer-readable storage media containing computer-executable instructions that, when executed on a computer, implement a method comprising:

serving a web page to a client over a distributed network;

receiving client input via the web page;

comparing the client input with multiple and distinct client input security screens stored in a security declarative module, wherein the security declarative module includes a global section configured to screen all types of client input values and an individual values section configured to screen particular types of client input values, wherein the global section is used to first screen one or more client input values and then the individual values section is used to screen at least one of the one or more client input values;

if invalid client input is detected, performing a screening action on the invalid client input as indicated by the security declarative module; and

wherein the client input security screens included in the security declarative module can be applied to multiple web pages.

22. (Canceled).

23. (Canceled).

24. (Previously Presented) The one or more computer-readable media as recited in claim 21, wherein the security declarative module further comprises a web.config file.

25. (Original) The one or more computer-readable media as recited in claim 21, wherein the screening action further comprises an action specified in a client input security screen.

26. (Original) The one or more computer-readable media as recited in claim 21, wherein the screening action further comprises a default action that is not required to be specified in a client input security screen.

27. (Original) The one or more computer-readable media as recited in claim 21, wherein the multiple web pages are included in a web project.

28. (Original) The one or more computer-readable media as recited in claim 21, wherein the multiple web pages are included in a web-based application.

(9) Evidence Appendix: None

(10) Related proceedings Appendix: None